



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11122293 A**(43) Date of publication of application: **30.04.99**

(51) Int. Cl. **H04L 12/54**
H04L 12/58
G06F 13/00
H04L 9/14

(21) Application number: **09280010**(71) Applicant: **SHARP CORP**(22) Date of filing: **14.10.97**(72) Inventor: **KIMURA YOSHINOBU**(54) **ELECTRONIC MAIL SERVER SYSTEM**

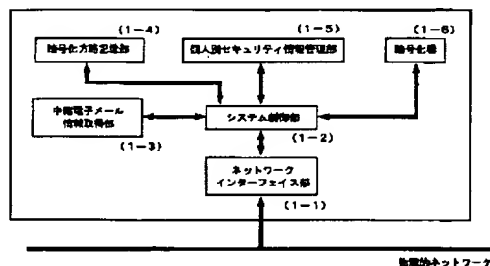
(57) Abstract:

PROBLEM TO BE SOLVED: To improve the security in the electronic mail server system.

SOLUTION: The electronic mail server system is provided with a communication network configured by using an ISDN, a public telephone line, the Ethernet or the like, a network interface section 1-1 that provides physical connection to the network, understands a protocol to make communication with an optional host connected to the communication network to control the communication, a relay electronic mail information acquisition section 1-3 that receives an electronic mail transferred from other computer via the network and acquires the information of the electronic mail, an individual security information management section 1-5 that stores an encryption scheme applied to the mail for each user of each electronic mail, an encryption scheme storage section 1-4 that stores a scheme to maintain the security in the entire organization in which mail servers are in existence, an encryption device 1-6 that encrypts the mail when it is discriminated that encryption is conducted by referring the individual security information management section 1-5 and the encryption scheme storage section 1-4 based on the information

obtained by the relay electronic mail information acquisition 1-3, and a system control section 1-2 that controls all the sections.

COPYRIGHT: (C)1999,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-122293

(43) 公開日 平成11年(1999) 4月30日

(51) Int.Cl.⁸

識別記号

F I

H 0 4 L 12/54

H 0 4 L 11/20

1 0 1 B

12/58

G 0 6 F 13/00

3 5 1 G

G 0 6 F 13/00

3 5 1

H 0 4 L 9/00

6 4 1

H 0 4 L 9/14

審査請求 未請求 請求項の数 7 O L (全 8 頁)

(21) 出願番号

特願平9-280010

(22) 出願日

平成9年(1997)10月14日

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 木村 吉伸

大阪府大阪市阿倍野区長池町22番22号 シ

ャープ株式会社内

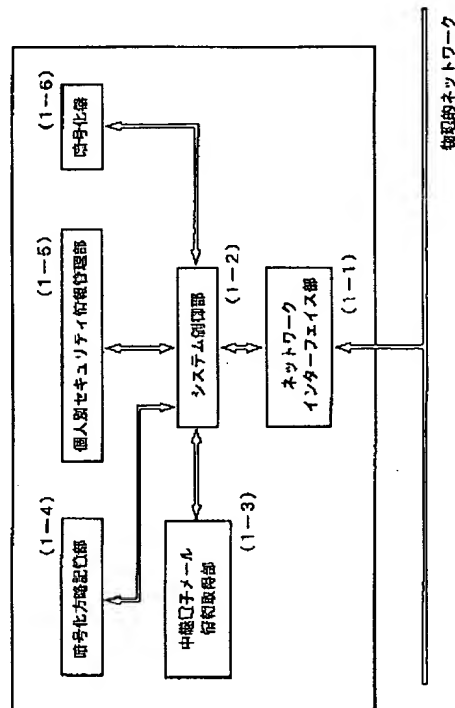
(74) 代理人 弁理士 梅田 勝

(54) 【発明の名称】 電子メールサーバシステム

(57) 【要約】

【課題】 電子メールサーバシステムにおいて、セキュリティを向上させる。

【解決手段】 ISDN、公衆電話回線、またはEthernetなどを用いて構成される通信ネットワークと、上記ネットワークに対して物理的接続を提供し、通信ネットワークに接続された任意のホストと通信を行う為のプロトコルを理解し通信を司るネットワークインターフェイス部と、上記ネットワークを介して他の計算機から転送された電子メールを受け、その電子メールの情報を取得する中継電子メール情報取得部と、各電子メールの利用者毎に、メールに対して行う暗号化方略を蓄積した個人別セキュリティ情報管理部とメールサーバの存在する組織全体におけるセキュリティを維持する為の方略を蓄積した暗号化方略記憶部と、上記中継電子メール情報取得部から得られた情報を基に個人別セキュリティ情報管理部と暗号化方略記憶部を参照することにより暗号化を行うと判断された場合にメールの暗号化を行う暗号化器と、上記すべての部分の制御を司るシステム制御部と、を備える。



【特許請求の範囲】

【請求項 1】 I S D N、公衆電話回線、または E t h e r n e t などを用いて構成される通信ネットワークと、上記ネットワークに対して物理的接続を提供し、通信ネットワークに接続された任意のホストと通信を行うためのプロトコルを理解し通信を司るネットワークインターフェイス部と、上記ネットワークを介して他の計算機から転送された電子メールを受け、その電子メールの情報を取得する中継電子メール情報取得部と、各電子メールの利用者毎に、メールに対して行う暗号化方略を蓄積した個人別セキュリティ情報管理部と、メールサーバの存在する組織全体におけるセキュリティを維持する為の方略を蓄積した暗号化方略記憶部と、上記中継電子メール情報取得部から得られた情報を基に個人別セキュリティ情報管理部と、暗号化方略記憶部を参照することにより暗号化を行うと判断された場合にメールの暗号化を行う暗号化器と、上記すべての部分の制御を司るシステム制御部とを備えたことを特徴とする電子メールサーバシステム。

【請求項 2】 請求項 1 に記載の電子メールサーバシステムにおいて、暗号化方略記憶部は、電子メールサーバが任意に決定可能なキーワード表を記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記キーワード表に示されたキーワードを含むと判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステム。

【請求項 3】 請求項 1 に記載の電子メールサーバシステムにおいて、暗号化方略記憶部は、電子メールサーバが任意に決定可能な電子メール利用者リストを記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記電子メール利用者リストに示された利用者の発信メールであると判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステム。

【請求項 4】 請求項 1 に記載の電子メールサーバシステムにおいて、暗号化方略記憶部は、電子メールサーバが任意に決定可能な電子メール配送宛先表を記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記電子メール配送宛先表に示された宛先に送信されるメールであると判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステム。

【請求項 5】 請求項 1 に記載の電子メールサーバシステムにおいて、暗号化方略記憶部は、電子メールサーバが任意に決定可能な電子メール配送宛先表及び、各配送宛先までの電子メールの通過経路とその経路のセキュリティレベルを記した表を記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記電子メー

ル配送宛先表に示された宛先に送信されるメールであると判断した場合、電子メールが宛先に着信するまでに通過する経路とその経路のセキュリティレベルを獲得し、それらの情報を基に電子メールを暗号化する必要があると判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステム。

【請求項 6】 請求項 1 に記載の電子メールサーバシステムにおいて、

暗号化方略記憶部は、電子メールサーバが任意に決定可能な発信時刻表を記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記電子メール発信時間表に示された宛先に送信されるメールであると判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステム。

【請求項 7】 請求項 1 に記載の電子メールサーバシステムにおいて、

中継電子メール情報取得部から得られたメールの付属情報中に、発信者が指定した暗号化依頼のキーワードが含まれていた場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、インターネット等のネットワークを用いてデータを送受信する機能を持つ計算機、および、送受信に使用する計算機（サーバ）に関する。

【0002】

【従来の技術】近年、Internet 等のようにネットワークを用いて遠隔地とデータの送受信を行う場合が増加し続けている。

【0003】Internet 等のネットワークシステムを使用してデータの送受信を行う場合、第三者によりネットワーク上でデータの盗聴、改竄、消去等されてしまう可能性がある。上記の Internet は複数の組織が提供するネットワークをルーター等を利用して接続し、大規模なネットワーク全体を構成している。

【0004】このネットワークを用いて任意の企業の所属員が、他の組織へ電子メールなどのデータを転送する場合、複数の組織のネットワーク上を経由する可能性は非常に高い。データが経由する組織では、ルータ等からネットワーク上に流れるデータを容易に読みとる事ができるという問題点がある。

【0005】上記の課題は送受信データの暗号化により解決される（特開平 9 - 4 6 3 3 0 号公報、特開平 6 - 2 7 6 2 2 号公報）。データ転送に適用可能な暗号化方式は、対象鍵暗号、公開鍵暗号、電子署名などがあり、既に複数のツールを使用することにより、データを容易に暗号化可能である。

【0006】

【発明が解決しようとする課題】しかし、送信者がネッ

3

トワークに送出する前に暗号化を施さなければ、受信側では上記の問題に対して対処法がない。

【0007】またネットワークを利用してデータの送受信を自組織以外と送受信する利用者は通常、そのデータがどの物理的経路を経由するかなどを意識する事は少ないので、送受信するデータのセキュリティに対する意識が低くなることも問題の一つである。ネットワーク通信におけるセキュリティへの関心が低い利用者一人のために、その個人が属する企業の機密が漏洩する危険がある。現在はその課題に対して、特に対策は講じられていない。

【0008】

【課題を解決するための手段】請求項1記載の電子メールサーバシステムは、ISDN、公衆電話回線、またはEthernetなどを用いて構成される通信ネットワークと、上記ネットワークに対して物理的接続を提供し、通信ネットワークに接続された任意のホストと通信を行う為のプロトコルを理解し通信を司るネットワークインターフェイス部と、上記ネットワークを介して他の計算機から転送された電子メールを受け、その電子メールの情報を取得する中継電子メール情報取得部と、各電子メールの利用者毎に、メールに対して行う暗号化方略を蓄積した個人別セキュリティ情報管理部とメールサーバの存在する組織全体におけるセキュリティを維持する為の方略を蓄積した暗号化方略記憶部と、上記中継電子メール情報取得部から得られた情報を基に個人別セキュリティ情報管理部と暗号化方略記憶部を参照することにより暗号化を行うと判断された場合にメールの暗号化を行う暗号化器と、上記すべての部分の制御を司るシステム制御部と、を備えたことを特徴とする電子メールサーバシステムである。

【0009】請求項2記載の電子メールサーバシステムは、請求項1に記載の電子メールサーバシステムにおいて、暗号化方略記憶部は、電子メールサーバが任意に決定可能なキーワード表を記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記キーワード表に示されたキーワードを含むと判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステムである。

【0010】請求項3記載の電子メールサーバシステムは、請求項1に記載の電子メールサーバシステムにおいて、暗号化方略記憶部は、電子メールサーバが任意に決定可能な電子メール利用者リストを記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記電子メール利用者リストに示された利用者の発信メールであると判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステムである。

【0011】請求項4記載の電子メールサーバシステムは、請求項1に記載の電子メールサーバシステムにおい

4

て、暗号化方略記憶部は、電子メールサーバが任意に決定可能な電子メール配送宛先表を記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記電子メール配送宛先表に示された宛先に送信されるメールであると判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステムである。

【0012】請求項5記載の電子メールサーバシステムは、請求項1に記載の電子メールサーバシステムにおいて、暗号化方略記憶部は、電子メールサーバが任意に決定可能な電子メール配送宛先表及び、各配送宛先までの電子メールの通過経路とその経路のセキュリティレベルを記した表を記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記電子メール配送宛先表に示された宛先に送信されるメールであると判断した場合、電子メールが宛先に着信するまでに通過する経路とその経路のセキュリティレベルを獲得し、それらの情報を基に電子メールを暗号化する必要があると判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステムである。

【0013】請求項6記載の電子メールサーバシステムは、請求項1に記載の電子メールサーバシステムにおいて、暗号化方略記憶部は、電子メールサーバが任意に決定可能な発信時刻表を記憶すると共に、システム制御部は、中継電子メール情報取得部から得られた情報から、上記電子メール発信時刻表に示された宛先に送信されるメールであると判断した場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステムである。

【0014】請求項7記載の電子メールサーバシステムは、請求項1に記載の電子メールサーバシステムにおいて、中継電子メール情報取得部から得られたメールの附属情報中に、発信者が指定した暗号化依頼のキーワードが含まれていた場合、暗号化器により暗号化を行う事の特徴とする電子メールサーバシステムである。

【0015】

【発明の実施の形態】以下、この発明を図示の形態により詳細に説明する。

【0016】図1は本実施の形態のセキュリティを考慮した電子メールサーバシステムのブロック図である。

【0017】電子メールサーバシステムは、ネットワークインターフェイス部(1-1)、システム制御部(1-2)、中継電子メール情報取得部(1-3)、暗号化方略記憶部(1-4)、個人別セキュリティ情報管理部(1-5)、暗号化器(1-6)から構成される。

【0018】本メールサーバは、Ethernet等のネットワークに接続(有線/無線に関わらず)されており、任意の通信プロトコル(TCP/IP, IPX等)を用いて、他の計算機とメールの送受信を行う。

【0019】ネットワーク上における本メールサーバシステムの位置付けの例を図2に示す。

【0020】図2の例では、本発明のメールサーバはEthernetでネットワークに接続され、メール送信のクライアントとして、同様のネットワークに接続された計算機(2-2)、及び無線通信路を用いてPPPなどで通信を行うモバイル環境の計算機(2-3)を持つ。

【0021】本発明のメールサーバ(2-1)から計算機(2-8)へメールを転送する場合、ネットワークアドレスの異なる複数のネットワークを経由する。すなわち、図2中では、Router(2-4~7)を中継点として転送される。ネットワークに対する物理的インターフェイスを、ネットワークインターフェイス部(1-1)が提供する。また、通信プロトコルに従って受信したデータからメールへ成形する機能も持つ。

【0022】インターフェイス部で得られたメールは、中継電子メール情報取得部において、発信者、送信先、送信日時、送信本文等を抽出され、システム制御部に転送される。システム制御部は、メールから附属情報を獲得すると共に、暗号化方略記憶部(1-4)から暗号化方略を得る。

【0023】暗号化方略の具体例を以下に示す。

【0024】暗号化方略として、“特定のキーワードがメールに含まれていた場合には、暗号化を行う”が設定されていた場合、同時に暗号化方略記憶部で任意に設定可能なキーワード表を保持する。

【0025】図3に、キーワード表の例を示す。

【0026】この設定によると、メールの本文中に“暗号”等のキーワードが含まれている場合、システム制御部は、メールを暗号化する必要があると判断する。

【0027】暗号化方略として、“特定の人物から発信されたメールには、暗号化を行う”が設定されていた場合、同時に暗号化方略記憶部では任意に設定可能な発信者リストを保持する。

【0028】図4に発信者リストの例を示す。

【0029】この設定によると、メールの発信者名が本リストに記載されている場合、システム制御部は、メールを暗号化する必要があると判断する。

【0030】暗号化方略として、“特定の人物へ発信されたメールには、暗号化を行う”が設定されていた場合、同時に暗号化方略記憶部では任意に設定可能な受信者リストを保持する。

【0031】図5に受信者リストの例を示す。

【0032】この設定によると、メールの受信者名(宛先)が本リストに記載されている場合、システム制御部は、メールを暗号化する必要があると判断する。

【0033】暗号化方略として、“特定の経路を用いて伝送されるメールには、暗号化を行う”が設定されていた場合、同時に暗号化方略記憶部では任意に設定可能な送信先リスト及びその宛先に至るまでの経路情報を保持する。

【0034】図6に経路情報リストの例を示す。

【0035】図6では経路情報と共に、その経路に対するセキュリティレベルの評価値を付記しておく。各経路に対して、どのような指標で評価を行うかはセキュリティ管理者に依る。図中の例では、経由するネットワークの数を評価値とし、値が小さい程、セキュリティレベルが高いとする。

【0036】また図6では、暗号化を行う必要のあるセキュリティレベルを示している。

10 【0037】本図ではセキュリティレベルが4以上の宛先へ送信するメールを暗号化する設定となっている。この例に従うと、YYY. ad. jp宛のメールを暗号化する必要があるとシステム制御部は判断する。暗号化方略として、“特定の時間に発信されるメールには、暗号化を行う”が設定されていた場合、同時に暗号化方略記憶部では任意に設定可能な暗号化時間リストを保持する。

【0038】図7に暗号化時間リストの例を示す。

20 【0039】この設定によると、メールの発信時間が本リストに記載されている場合、システム制御部は、メールを暗号化する必要があると判断する。

【0040】暗号化方略として、“発信者が、暗号必要であると明記したメールには、暗号化を行う”が設定されていた場合、システム制御部は、メールを暗号化する必要があると判断する。

【0041】図8に発信者が暗号化の必要性を明記したメールの例を示す。

【0042】本例では、Encryptionフィールドにより指定されている。中継電子メール情報取得部から得られた付属情報と、暗号化方略記憶部に蓄積された方略を参照することにより、暗号化が必要ないとシステム制御部が判断した場合、メールは暗号化処理を加えられることなくメールサーバから送出される。

【0043】メールの暗号化処理が必要であるとシステム制御部が判断した場合、システム制御部は個人別セキュリティ情報取得部から、該メールの発信者に関する情報を取得する。

【0044】図9に個人別セキュリティ情報の例を示す。

40 【0045】本情報には、発信者アドレスと各発信者毎に指定された暗号化方式、また必要であれば、その暗号化方式における暗号化鍵が示されている。

【0046】図10に処理のフローチャートを示す。

【0047】システム制御部は個人別セキュリティ情報取得部から獲得した情報をもとに暗号化器を1駆動する(S1~S5)。暗号化器では、個人別セキュリティ情報取得部に示された暗号化方式に対する全ての暗号化機構を備える。暗号化処理が完了すると、メールはメールサーバから送出される(S6~S8)。

50 【0048】

【発明の効果】請求項 1 に係る電子メールサーバシステムは、Ethernet 等に物理的に接続された他のクライアントから送信されたメールをネットワークインターフェイス部から取得し、中継電子メール情報取得部が取得した該データの各種情報（送信先など）と、暗号化方略記憶部に蓄積された暗号化の方針と、個人別セキュリティ情報管理部に設定されたセキュリティに関する設定を参照することによりシステム制御部が該データに対してどの暗号化を行うかを決定し、その決定に基づき暗号化器が暗号化を行う。暗号化されたデータは再びネットワークを介して送出される。以上の機構により、データ送信者が特に意識することなく、もしくはメール送信者に関係なくネットワーク管理者がネットワークからの機密漏洩を防ぐことが可能となる。

【0049】請求項 2 に係る電子メールサーバシステムは、請求項 1 の効果に加えて、暗号化方略記憶部において、ネットワークもしくはセキュリティ管理者が自由に設定可能なキーワード表を記憶することにより、該メールにキーワードが含まれていた場合のみ、該メールの暗号化を行う。条件に合ったメールのみに暗号化処理を行い、その他については処理を施さないことにより、計算機能力の無駄を防ぐ効果がある。

【0050】請求項 3 に係る電子メールサーバシステムは、請求項 1 の効果に加えて、暗号化方略記憶部において、ネットワークもしくはセキュリティ管理者が自由に設定可能な発信者名表もしくはメールアドレスリストにより、該メールの発信者がリストに記憶されていた場合のみ該メールの暗号化を行う。条件に合ったメールのみに暗号化処理を行い、その他については処理を施さないことにより、計算機能力の無駄を防ぐ効果がある。

【0051】請求項 4 に係る電子メールサーバシステムは、請求項 1 の効果に加えて、暗号化方略記憶部において、ネットワークもしくはセキュリティ管理者が自由に設定可能な送信先もしくは送信先アドレスリストにより、該メールの送信先がリストに記憶されていた場合のみ該メールの暗号化を行う。条件に合ったメールのみに暗号化処理を行い、その他については処理を施さないことにより、計算機能力の無駄を防ぐ効果がある。

【0052】請求項 5 に係る電子メールサーバシステムは、請求項 1 の効果に加えて、暗号化方略記憶部において、ネットワークもしくはセキュリティ管理者が自由に設定可能な送信先及び、送信先に至るまでの伝送経路を記憶し、かつ各通信経路毎に経路のセキュリティレベルも同様に記憶し、該メールの伝送経路のセキュリティレベルが任意に設定可能なしきい値よりも低い場合のみ該メールの暗号化を行う。条件に合ったメールのみに暗号化処理を行い、その他については処理を施さないことに

より、計算機能力の無駄を防ぐ効果がある。

【0053】請求項 6 に係る電子メールサーバシステムは、請求項 1 の効果に加えて、暗号化方略記憶部において、ネットワークもしくはセキュリティ管理者が自由に設定可能な暗号化時間リストにより、条件に合ったメールのみに暗号化処理を行い、その他については処理を施さないことにより、計算機能力の無駄を防ぐ効果がある。

【0054】請求項 7 に係る電子メールサーバシステムは、請求項 1 の効果に加えて、メールの発信者に暗号化を指定可能な記述を許すことで、メールサーバでの暗号化処理を可能にする。よって、メール発信者の計算機に負荷をかけることなく、メールの暗号化を行う効果がある。

【図面の簡単な説明】

【図 1】本発明のセキュリティを考慮した電子メールサーバシステムブロック図である。

【図 2】本発明のメールサーバの通信ネットワーク上における位置関係を示す図である。

【図 3】暗号化の必要性を判断するためのキーワード表である。

【図 4】暗号化の必要性を判断するための発信者リストである。

【図 5】暗号化の必要性を判断するための受信者リストである。

【図 6】暗号化の必要性を判断するための経路情報リストである。

【図 7】暗号化の必要性を判断するための暗号化時間リストである。

【図 8】発信者による暗号化依頼の例である。

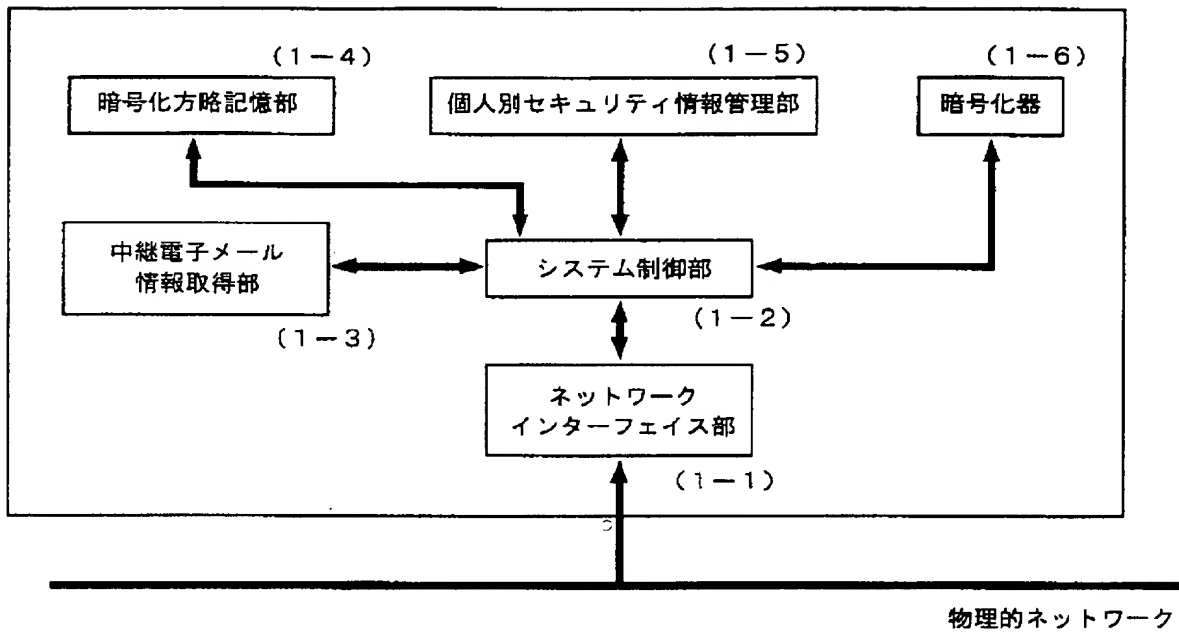
【図 9】個人別セキュリティ情報の例である。

【図 10】本発明の処理を示すフローチャートである。

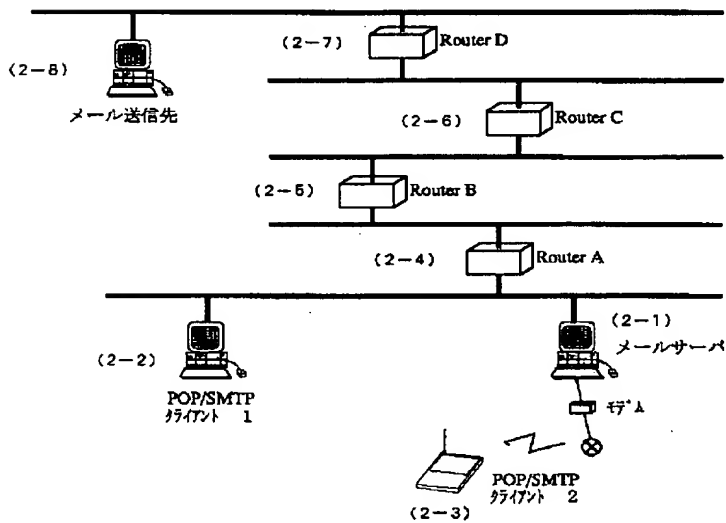
【符号の説明】

- 1-1 ネットワークインターフェイス部
- 1-2 システム制御部
- 1-3 中継電子メール情報取得部
- 1-4 暗号化方略記憶部
- 1-5 個人別セキュリティ情報管理部
- 1-6 暗号化器
- 2-1 メールサーバ装置
- 2-2 POP/SMT Pクライアント
- 2-3 POP/SMT Pクライアント
- 2-4 Router
- 2-5 Router
- 2-6 Router
- 2-7 Router

【図 1】



【図 2】



【図 3】

機密 セキュリティ 暗号 パスワード 鍵 シークレット
 privacy authentication

【図 7】

暗号化: 8:30~12:15
 13:10~17:10

【図 4】

sasa@AAAA.sharp.co.jp
 bbbb@BBBB.sharp.co.jp
 cccc@CCCC.sharp.co.jp
 dddd@DDDD.sharp.co.jp

【図 5】

suzuki@WWW.co.jp
 satoh@XXXX.co.jp
 yamada@YYYY.ad.jp
 minami@ZZZZ.co.jp

【図6】

送信先	伝送経路	セキュリティレベル
WWW.co.jp	aaa.bbb.bbb.bbb 111.111.111.111 www.www.www.www	3
XXXX.co.jp	111.111.111.111 mmm.mmm.mmm	2
YYYY.ad.jp	ddd.ddd.ddd.ddd eee.eee.eee.eee fff.fff.fff.fff ggg.ggg.ggg.ggg	4
ZZZZ.co.jp	111.111.111.111 111.111.111.111	2

暗号化境界レベル：4

【図8】

From : oooooo@yyy.sharp.co.jp
 Subject: Secret mail
 Date: Tue, 18 Mar 1997 16:07:27 +0900
 Sender: yyyyyy@zzz.sharp.co.jp
 Encryption: on

【図9】

個人名	暗号化方式	暗号化値
aaaa@AAAA.sharp.co.jp	PEM	FDASFASDCX...
bbbb@BBBB.sharp.co.jp	MOSS
cccc@CCCC.sharp.co.jp	FJPEM
dddd@DDDD.sharp.co.jp	PGP
.....

【図10】

